AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1-3. (Canceled)

4. (Previously Presented) The terminal according to claim 22, wherein the key for the encrypted cryptographic algorithm is a key for secret key cryptography.

5. (Previously Presented) The terminal according to claim 22, wherein the key for the encrypted cryptographic algorithm is a key for public key cryptography.

6. (Canceled)

7. (Previously Presented) The terminal according to claim 22, wherein said control section instructs said cryptographic algorithm storage section to output a requested cryptographic algorithm upon receiving a transmission request for any one of the cryptographic algorithms stored in said cryptographic algorithm storage section, and

said encryption/decryption section encrypts the requested cryptographic algorithm as the information to be transmitted.

8. (Previously Presented) The terminal according to claim 22, wherein when a partner with which said terminal communicates is an apparatus including said cryptographic communication terminal, said terminal:

requests the partner for a new cryptographic algorithm and/or a key for a corresponding encrypted algorithm;

decrypts a corresponding response by using said encryption/decryption section;

stores the requested cryptographic algorithm in said cryptographic algorithm storage section upon receiving the cryptographic algorithm; and

stores the requested key for the encrypt algorithm in said key information storage section upon receiving the key.

9. (Currently Amended) A cryptographic communication center apparatus ~~comprising~~ communicating with said cryptographic communication terminal defined in claim 22, wherein when the algorithm decryption key is requested from [[the]] a partner of the cryptographic communication center apparatus, said apparatus inputs the corresponding algorithm decryption key as the information to be transmitted to the partner to said encryption/decryption section.

10. (Previously Presented) The apparatus according to claim 9, wherein:

said apparatus comprises said cryptographic communication terminal and an update cryptographic algorithm storage section for storing a plurality of types of cryptographic algorithms decrypted by using a key for the encrypted algorithm; and

said control section, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructs said update cryptographic algorithm storage section, in place of said cryptographic algorithm storage section, to output the requested cryptographic algorithm as the information to be transmitted.

11. (Previously Presented) The apparatus according to claim 9, further comprising a key encryption section for, when the key for the encrypted algorithm is requested from said cryptographic communication terminal, encrypting the key for the encrypted algorithm to be transmitted, and inputting the encrypted key for the encrypted algorithm, as the information to be transmitted, to said encryption/decryption section.

12. (Previously Presented) The apparatus according to claim 11, wherein said key encryption section encrypts the key for the encrypted algorithm by using a key unique to a cryptographic communication terminal of the partner.

13. (Previously Presented) A cryptographic communication system comprising not less than two cryptographic communication terminals each defined in claim 22.

14-16. (Canceled)

17. (Previously Presented) The storage according to claim 23, wherein:

said control section further comprises a program for, when a transmission request for any of the cryptographic algorithms stored in said cryptographic algorithm storage section is received, instructing said cryptographic algorithm storage section to output the requested cryptographic algorithm; and

said encryption/decryption section further comprises a program for encrypting the requested cryptographic algorithm as the information to be transmitted.

18. (Previously Presented) A storage according to claim 23, further comprising a program for, when a key for the encrypted algorithm is requested from the partner, inputting the corresponding key for the encrypted algorithm, as the information to be transmitted to the partner, to said encryption/decryption section.

19. (Previously Presented) A cryptographic communication center apparatus having said storage medium defined in claim 23, comprising:

an updated cryptographic algorithm storage section for storing a plurality of types of cryptographic algorithms encrypted by the key for the encrypted algorithm; and

means for, when the cryptographic algorithm decryption key is requested from the partner, inputting a corresponding key for the encrypted algorithm, as information to be transmitted to the partner, to said encryption/decryption section,

wherein said control section stores a program for, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructing said

update cryptographic algorithm storage means to output the requested cryptographic algorithm as the information to be transmitted.

20. (Currently Amended) ~~The system according to claim 13,~~

A cryptographic communication system comprising not less than two cryptographic communication terminals each defined in claim 22 and a cryptographic communication center apparatus communicating with a cryptographic communication terminal of the cryptographic communication system,

wherein when the algorithm decryption key is requested from a partner of the cryptographic communication center apparatus, said cryptographic communication center apparatus inputs the corresponding algorithm decryption key as the information to be transmitted to the partner to said encryption/decryption section; and said cryptographic communication terminal acquires the cryptographic algorithm and a decryption key therefor from said cryptographic communication center apparatus.

21. (Previously Presented) The system according to claim 11, wherein said cryptographic communication terminal acquires a cryptographic algorithm from another cryptographic communication terminal and acquires a corresponding decryption key from said cryptographic communication center apparatus.

22. (Previously Presented) A cryptographic communication terminal comprising:

a control section for designating an encrypted cryptographic algorithm and an encrypted encryption/decryption key to be used in the cryptographic communication based on identification information;

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication in encrypted form, and outputting the encrypted cryptographic algorithm designated by the control section;

a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm;

a key information decryption section for decrypting the encrypted encryption/decryption key used for cryptographic communication and the encrypted key used for decrypting the encrypted cryptographic algorithm to create an encryption/decryption key used for cryptographic communication and an decryption key for decrypting the encrypted cryptographic algorithm;

a cryptographic algorithm decryption section for decrypting the encrypted cryptographic algorithm to generate an cryptographic algorithm by using the decryption key for decrypting the encrypted cryptographic algorithm; and

an encryption/decryption section for encrypting/decrypting communication messages by using the cryptographic algorithm and the encryption/decryption key used for cryptographic communication.

23. (Previously Presented) A computer readable medium storing a program for implementing:

a control section for designating an encrypted cryptographic algorithm and an encrypted encryption/decryption key to be used in the cryptographic communication based on identification information;

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication in encrypted form, and outputting the encrypted cryptographic algorithm designated by the control section;

a key information storage section for storing and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm;

a key information decryption section for decrypting the encrypted encryption/decryption key used for cryptographic communication and the encrypted key used for decrypting the encrypted cryptographic algorithm to create an encryption/decryption key used for cryptographic communication and an decryption key for decrypting the encrypted cryptographic algorithm;

a cryptographic algorithm decryption section for decrypting the encrypted cryptographic algorithm to generate an cryptographic algorithm by using the decryption key for decrypting the encrypted cryptographic algorithm; and

an encryption/decryption section for encrypting/decrypting communication messages by using the cryptographic algorithm and the encryption/decryption key used for cryptographic communication.

24. (Previously Presented) The terminal according to claim 22, further comprising:

an ID storage section for storing the identification information.

25. (Canceled)